

Alert Bulletin

Bulletin N.: 54

Publication Date: 26/06/2025

Subject: Alerta 2025-54 Vulnerabilidades críticas en Cisco ISE

Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

- Motor de servicios de identidad de Cisco (ISE)
- Conector de identidad pasiva de Cisco ISE (ISE-PIC)
- Versiones:
 - CVE-2025-20281: ISE/ISE-PIC 3.3 y posteriores
 - CVE-2025-20282: ISE/ISE-PIC 3.4 únicamente

Descripción

Cisco ha revelado dos vulnerabilidades **críticas** en sus productos **Identity Services Engine (ISE)** e **ISE Passive Identity Connector (ISE-PIC)**. Estas fallas, identificadas como **CVE-2025-20281** y **CVE-2025-20282**, permiten a un atacante **remoto y no autenticado** ejecutar comandos arbitrarios en los dispositivos afectados **con privilegios de root**, lo que implica un **control total sobre el sistema operativo subyacente**.

Ambas vulnerabilidades han recibido una calificación máxima de **CVSS 10.0**, lo que las convierte en amenazas de alto impacto para las organizaciones que utilizan estas soluciones de Cisco en entornos de autenticación, control de acceso y monitoreo de identidad.

CVE-2025-20281- Ejecución remota de código mediante API maliciosa

Esta falla afecta a las versiones **3.3 y posteriores** de Cisco ISE e ISE-PIC. Se trata de un error en la validación de entradas en una API específica, lo que permite a un atacante enviar solicitudes especialmente diseñadas que no requieren autenticación previa.

Al recibir estas solicitudes, el sistema ejecuta los comandos incluidos con privilegios **administrativos máximos (root)**, comprometiendo completamente la integridad y seguridad del dispositivo.

CVE-2025-20282 – Carga y ejecución de archivos maliciosos

Esta vulnerabilidad afecta únicamente a la versión **3.4 de Cisco ISE e ISE-PIC**.
En este caso, el problema radica en que el sistema **no verifica adecuadamente los archivos cargados por el usuario**. Un atacante remoto puede aprovechar esta falla para **subir archivos maliciosos** y ubicarlos en directorios privilegiados del sistema.
Una vez cargados, los archivos pueden ser ejecutados con privilegios de root, dando acceso completo al atacante.

Ambas vulnerabilidades son **independientes entre sí**, por lo que un sistema puede estar afectado por una, ambas

Solución:

Se recomienda a los clientes actualizar a una **versión de software fija** adecuada como se indica en la siguiente tabla:

Cisco ISE or ISE-PIC Release	First Fixed Release for CVE-2025-20281	First Fixed Release for CVE-2025-20282
3.2 and earlier	Not vulnerable	Not vulnerable
3.3	3.3 Patch 6 ise-apply- CSCwo99449_3.3.0.430_patch4- SPA.tar.gz	Not vulnerable
3.4	3.4 Patch 2 ise-apply- CSCwo99449_3.4.0.608_patch1- SPA.tar.gz	3.4 Patch 2 ise-apply-CSCwo99449_3.4.0.608_patch1- SPA.tar.gz

Para obtener instrucciones sobre cómo actualizar un dispositivo, consulte las Guías de actualización en la página de soporte de **Cisco Identity Service Engine** .

Información adicional:

- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-unauth-rce-ZAd2GnJ6>
- <https://www.cisco.com/c/en/us/support/security/identity-services-engine/series.html>
- <https://thehackernews.com/2025/06/critical-rce-flaws-in-cisco-ise-and-ise.html>